

**UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF PENNSYLVANIA**

JORDAN SACKS,

1255 25th Street, Apt. 324
Washington, DC 20037,

MICHAELLA KATZ,

7701 Atlantic Ave., Unit 33
Margate, NJ 08402,

and

AMANDA GARTHWAITE,

289 Forbes Court
Warrenton, VA 20186,

on behalf of themselves and all others similarly situated,

Plaintiffs,

v.

WAWA, INC.,

260 W. Baltimore Pike
Wawa, Pennsylvania 19063

Defendant.

Civil Action No.

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiffs Jordan Sacks, Michaella Katz, and Amanda Garthwaite (“Plaintiffs”), individually and on behalf of a class of all those similarly situated (the “Class” or “Class Members”), upon personal knowledge of the facts pertaining to Plaintiffs and on information and belief as to all other matters, and upon the investigation conducted by Plaintiffs’ counsel, file this civil action against defendant Wawa, Inc. (“Wawa”), and alleges as follows:

SUMMARY OF THE CASE

1. Wawa is a privately-held corporation that operates over 850 convenience stores in six states and the District of Columbia. It claims over \$12 billion in annual revenue, and claims to serve over 700 million customers annually.¹

2. On December 19, 2019, Wawa revealed that it had discovered malicious software (“malware”) on Wawa payment processing servers. According to Wawa, “[t]his malware affected customer payment card information used at potentially all Wawa locations beginning at different points in time after March 4, 2019 and until it was contained” on December 12, 2019.

3. Plaintiffs bring this class action on behalf of a nationwide class against Wawa because of its failure to protect the confidential information of millions of its customers—including credit and debit card numbers, expiration dates, and cardholder names on payment cards (collectively, “Financial Information”). Wawa’s wrongful disclosure (the “Data Breach”) has harmed Plaintiffs and the Class.

JURISDICTION AND VENUE

4. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d)(2), because this is a class action in which the matter in

¹ Ellie Silverman, *Wawa is undergoing a huge expansion, from grain bowls to fair-trade coffee to catering*, Philadelphia Inquirer, Apr. 4, 2019.

controversy exceeds the sum of \$5,000,000, there are more than 100 proposed Class Members, and minimal diversity exists as Defendant is a citizen of a state different from that of at least one Class Member.

5. This Court has personal jurisdiction over Wawa because it is headquartered in this district, registered and regularly conducts business in Pennsylvania, and has sufficient minimum contacts in Pennsylvania such that Wawa intentionally avails itself of this Court's jurisdiction by conducting operations here and contracting with companies in this District.

6. Venue is proper in this District pursuant to 28 U.S.C. § 1391, because a substantial part of the events or omissions giving rise to the conduct alleged herein occurred in, were directed to, and/or emanated from this District. Venue is additionally proper because Wawa transacts business and may be found in this District.

PARTIES

7. Plaintiff Jordan Sacks is an individual residing in Washington, DC, who has been a customer of Wawa, and whose Financial Information, on information and belief, was compromised in the Data Breach described herein. Mr. Sacks has been aware of the Data Breach since shortly after its disclosure, and has since invested substantial time in reviewing his statements and transactions to attempt to determine whether he has been victimized as a result of the Data Breach. Mr. Sacks is not yet aware of whether that is the case, and has reason to be concerned about the security of his Financial Information until that is determined.

8. Plaintiff Michaella Katz is an individual residing in Margate, New Jersey, who has been a customer of Wawa, and whose Financial Information, on information and belief, was compromised in the Data Breach described herein. Ms. Katz has been aware of the Data Breach since shortly after its disclosure, and has since invested substantial time in reviewing her

statements and transactions to attempt to determine whether she has been victimized as a result of the Data Breach. Ms. Katz is not yet aware of whether that is the case, and has reason to be concerned about the security of her Financial Information until that is determined.

9. Plaintiff Amanda Garthwaite is an individual residing in Warrenton, Virginia, who has been a customer of Wawa, and whose Financial Information, on information and belief, was compromised in the Data Breach described herein. Ms. Garthwaite has been aware of the Data Breach since shortly after its disclosure, and has since invested substantial time in reviewing her statements and transactions to attempt to determine whether she has been victimized as a result of the Data Breach. Ms. Garthwaite is not yet aware of whether that is the case, and has reason to be concerned about the security of her Financial Information until that is determined.

10. Defendant Wawa, Inc. (“Wawa”) is a privately-owned New Jersey corporation with its principal place of business in Wawa, Pennsylvania.

FACTUAL BACKGROUND

11. Wawa owns and operates more than 850 convenience retail stores in Pennsylvania, New Jersey, Delaware, Maryland, Virginia, Florida, and Washington, D.C. Wawa is the largest convenience store chain in Greater Philadelphia, and it is also the third-largest retailer of food in Greater Philadelphia.

12. According to Wawa, “at different points in time after March 4, 2019, malware began running on in-store payment processing systems at potentially all Wawa locations.” The malware “was present on most store systems by approximately April 22, 2019.” But Wawa did not discover the malware for over nine months after it initially infected Wawa’s systems, and did not disclose the Data Breach for over a week after that.

13. Wawa believes “this malware no longer poses a risk to customers using payment cards at Wawa.” However, that assessment does not account for the possibility that Wawa customers whose data has been improperly accessed have been or will be victimized by fraud and/or identity theft resulting from the Data Breach.

14. Wawa had obligations, arising from promises made to its customers like Plaintiffs and other Class Members, and based on industry standards, to keep the Financial Information confidential and to protect it from unauthorized disclosures. Class Members provided their Financial Information to Wawa with the understanding that Wawa and any business partners to whom Wawa disclosed the Financial Information would comply with their obligations to keep such information confidential and secure from unauthorized disclosures.

15. Wawa claims it “is fully committed to data security.” It further claims to “use security techniques on” its websites, “and through or in connection with our mobile apps or other software- and Internet-enabled programs and services sponsored by Wawa (the ‘Sites’) to help protect against the loss, misuse or alteration of information collected from [its customers] at the Sites.” As Wawa puts it when customers “access [their] account information or transmit personally identifiable data to the Sites, that information is stored on servers that the Sites have attempted to secure from unauthorized access or intrusion. ‘Secure Socket Layer’ software encrypts personal information [its customers] transmit to the Sites.”²

16. However, Secure Socket Layer (“SSL”) encryption protects information only in the course of its transmission, and not upon its storage on Wawa systems. Moreover, SSL

² Wawa Official Privacy Policy, available at <https://www.wawa.com/privacy>.

encryption “is not sufficiently secure.”³ Wawa has disclosed no further detail about its efforts to secure its customers’ data prior to the Data Breach.

17. Wawa’s security failure demonstrates that it failed to honor its duties and promises by not:

- a. maintaining an adequate data security system to reduce the risk of data breaches and cyber-attacks;
- b. adequately monitoring its system to identify the data breaches and cyber-attacks; and
- c. adequately protecting Plaintiffs’ and the Class’s Financial Information.

18. Plaintiffs and other Class Members have been injured by the disclosure of their Financial Information in the Data Breach.

19. Plaintiffs and other Class Members would not have provided their Financial Information to Wawa had they known that Wawa did not take reasonable and necessary precautions to secure that information.

20. Wawa’s data security obligations and promises were particularly important given the substantial increase in data breaches, which were widely known to the public and to anyone in Wawa’s industry.

21. The United States Government Accountability Office noted in a June 2007 report on Data Breaches (“GAO Report”) that identity thieves use identifying data such as Social Security Numbers to open financial accounts, receive government benefits and incur charges and

³ See Internet Engineering Task Force, Deprecating Secure Sockets Layer Version 3.0, available at <https://tools.ietf.org/html/rfc7568>.

credit in a person's name.⁴ As the GAO Report states, this type of identity theft is the most harmful because it often takes some time for the victim to become aware of the theft, and the theft can impact the victim's credit rating adversely.

22. In addition, the GAO Report states that victims of identity theft will face "substantial costs and inconveniences repairing damage to their credit records" and their "good name."⁵

23. Identity theft victims frequently are required to spend many hours and large amounts of money repairing the impact to their credit. Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and/or bank/finance fraud.

24. There may be a time lag between when Financial Information is stolen and when it is used. According to the GAO Report:

[L]aw enforcement officials told us that in some cases, *stolen data may be held for up to a year or more before being used to commit identity theft*. Further, once stolen data have been sold or posted on the Web, *fraudulent use of that information may continue for years*. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.⁶

25. With access to an individual's Financial Information, criminals can do more than just empty a victim's bank account—they can also commit all manner of fraud, including obtaining a driver's license or official identification card in the victim's name but with the thief's picture. In addition, identity thieves may obtain a job, rent a house, or receive medical services in

⁴ See U.S. Gov't Accountability Off., GAO-07-737, *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent Is Unknown* (2007).

⁵ *Id.*, at 2, 9.

⁶ *Id.*, at 29 (emphasis added).

the victim's name. Identity thieves may even give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.⁷

26. Financial Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years. As a result of recent large-scale data breaches, identity thieves and cyber-criminals have openly posted stolen credit card numbers, and other Financial Information directly on various Internet websites making the information publicly available.

27. Indeed, data breaches and identity theft have a crippling effect on individuals and detrimentally impact the entire economy as a whole. Financial databases are especially valuable to identity thieves.

DAMAGE TO PLAINTIFFS AND CLASS MEMBERS

28. Plaintiffs and Class Members have been damaged by the of their Financial Information in the Data Breach.

29. Class Members face a substantial and imminent risk of fraudulent charges on their credit and debit cards. Whoever stole their Financial Information did so with the intent to use it for fraudulent purposes and/or to sell it to others with similar intentions.

30. Many Class Members have unknowingly already experienced, or will soon experience fraudulent credit and debit card purchases as a result of the Data Breach.

31. Yet more Class Members will incur out-of-pocket costs and expend time arranging for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, fees for replacement cards, and similar costs as a result of the Data Breach.

⁷ See *Warning Signs of Identity Theft*, Federal Trade Commissions, <https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft> (last accessed July 29, 2019).

32. Plaintiffs and Class Members also suffered “benefit of the bargain” damages. Class Members paid Wawa for goods with the legitimate expectation that their payments would be directed in part towards adequate data security. Wawa did not provide Class Members with such security.

33. Plaintiffs and Class Members have spent and will continue to spend substantial amounts of time monitoring their credit and debit card accounts for fraud, disputing fraudulent transactions, and reviewing their financial affairs more closely than they otherwise would have but for the Data Breach. Plaintiffs and Class Members will also spend time disputing fraudulent charges, obtaining replacement cards, and updating the card information they have stored with merchants other than Wawa. These efforts are burdensome and time-consuming.

34. Wawa has acknowledged that Plaintiffs and Class Members face a heightened risk of identity theft as a result of the Data Breach. Wawa instructed all affected customers to: (i) review their credit and debit card statements carefully to identify fraudulent transactions; (ii) obtain copies of their credit reports to “look for any inaccuracies and/or accounts [they] don’t recognize”; (iii) place a “fraud alert” on their credit files to “protect [them] against the possibility of an identity thief opening new credit accounts in [their] names”; and (iv) place a “security freeze” on their credit files to prevent creditors from accessing those files without their consent. Those instructions reflect Wawa’s understanding that Plaintiffs and Class Members face risks beyond fraudulent credit and debit card transactions.

WAWA VIOLATED THE FTC ACT

35. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, prohibits “unfair . . . practices in or affecting commerce.” The FTC has held that the failure to employ reasonable

measures to protect against unauthorized access to confidential consumer data constitutes an unfair act or practice prohibited by Section 5.

36. Various FTC publications and orders also form the basis of Wawa's duty. The FTC published guidance establishing reasonable data security practices for businesses. The FTC guidance provides that businesses should, among other things: protect the personal customer information they acquire; properly dispose of personal information that is not necessary to maintain; encrypt information stored on computer networks; understand their network's vulnerabilities; and install vendor-approved updates to address those vulnerabilities. FTC guidance also recommends that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating that someone may be trying to penetrate the system; and watch for large amounts of data being transmitted from the system.

37. Wawa violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect Financial Information and not complying with industry standards.

CLASS ALLEGATIONS

38. Pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3), as applicable, and (c)(4), Plaintiffs seek certification of the following Nationwide Class (the "Class") defined as follows:

All persons in the United States whose Financial Information was maintained on the servers of Wawa that were compromised as a result of the breach announced by Wawa on December 19, 2019.

39. Pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3), as applicable, and (c)(4), Plaintiff Jordan Sacks seeks certification of District of Columbia claims on behalf of a District of Columbia subclass, defined as follows:

All natural persons residing in the District of Columbia whose Financial Information was compromised in the Data Breach.

40. Pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3), as applicable, and (c)(4), Plaintiff Michaella Katz seeks certification of New Jersey claims on behalf of a New Jersey subclass, defined as follows:

All natural persons residing in New Jersey whose Financial Information was compromised in the Data Breach.

41. Pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3), as applicable, and (c)(4), Plaintiff Amanda Garthwaite seeks certification of Virginia claims on behalf of a Virginia subclass, defined as follows:

All natural persons residing in Virginia whose Financial Information was compromised in the Data Breach.

42. The Class and Subclasses are so numerous that joinder of all members is impracticable. On information and belief, the Class and Subclasses have several million members. Moreover, the disposition of the claims of the Class and Subclasses in a single action will provide substantial benefits to all parties and the Court.

43. There are numerous questions of law and fact common to Plaintiffs and Class Members. These common questions of law and fact include, but are not limited to, the following:

- a. Whether Wawa's data security systems prior to the Data Breach complied with all applicable legal requirements;
- b. Whether Wawa's data security systems prior to the Data Breach met industry standards;
- c. Whether Plaintiffs' and other Class members' Financial Information was compromised in the Data Breach; and

d. Whether Plaintiffs and other Class members are entitled to damages as a result of Wawa's conduct.

44. Plaintiffs' claims are typical of the claims of the Class's claims. Plaintiffs suffered the same injury as Class Members – *i.e.* upon information and belief, Plaintiffs' Financial Information was compromised in the Data Breach.

45. Plaintiffs will fairly and adequately protect the interests of the Class and Subclasses. Plaintiffs have retained competent and capable attorneys with significant experience in complex and class action litigation, including data breach class actions. Plaintiffs and their counsel are committed to prosecuting this action vigorously on behalf of the Class and have the financial resources to do so. Neither Plaintiffs nor their counsel have interests that are contrary to or that conflict with those of the proposed Class and Subclasses.

46. Wawa has engaged in a common course of conduct toward Plaintiffs and other Class and Subclass Members. The common issues arising from this conduct that affect Plaintiffs and Class and Subclass Members predominate over any individual issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

47. A class action is the superior method for the fair and efficient adjudication of this controversy. Class Members' interests in individually controlling the prosecution of separate actions are low given the magnitude, burden, and expense of individual prosecutions against large corporations such as Wawa. It is desirable to concentrate this litigation in this forum to avoid burdening the courts with individual lawsuits. Individualized litigation presents a potential for inconsistent or contradictory judgments, and also increases the delay and expense to all parties and the court system presented by the legal and factual issues of this case. By contrast, the class action procedure here will have no management difficulties. Wawa's records and the

records available publicly will easily identify the Class Members. The same common documents and testimony will be used to prove Plaintiffs' claims.

48. A class action is appropriate under Fed. R. Civ. P. 23(b)(2) because Wawa has acted or refused to act on grounds that apply generally to Class and Subclass Members, so that final injunctive relief or corresponding declaratory relief is appropriate as to all Class and Subclass Members.

FIRST COUNT

NEGLIGENCE

On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, on Behalf of Plaintiffs and the Statewide Subclasses

49. Plaintiffs reallege and incorporate by reference all preceding factual allegations.

50. Wawa required Plaintiffs and Class Members to submit non-public Financial Information to pay for goods and services via the Sites.

51. By collecting and storing this data, and sharing it and using it for commercial gain, Wawa had a duty of care to use reasonable means to secure and safeguard this Financial Information, to prevent disclosure of the information, and to guard the information from theft.

52. Wawa's duty included a responsibility to implement a process by which it could detect a breach of its security systems in a reasonably expeditious period of time and give prompt notice to those affected in the case of a data breach.

53. Wawa also owed a duty of care to Plaintiffs and members of the Class to provide security consistent with industry standards and the other requirements discussed herein, and to ensure that its systems and networks and the personnel responsible for them adequately protected their customers' Financial Information.

54. Only Wawa was in a position to ensure that its systems were sufficient to protect against the harm to Plaintiffs and the members of the Class from a data breach.

55. Wawa breached its duty by failing to use reasonable measures to protect Plaintiffs' and Class Members' Financial Information.

56. The specific negligent acts and omissions committed by Wawa include, but are not limited to, the following:

- a. failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiffs' and Class Members' Financial Information;
- b. failing to adequately monitor the security of its networks and systems;
- c. allowing unauthorized access to Plaintiffs' and Class Members' Financial Information; and
- d. failing to recognize in a timely manner that Plaintiffs' and other Class Members' Financial Information had been compromised.

57. It was foreseeable that Wawa's failure to use reasonable measures to protect and monitor the security of Financial Information would result in injury to Plaintiffs and other Class Members. Further, the breach of security, unauthorized access, and resulting injury to Plaintiffs and the members of the Class were reasonably foreseeable.

58. It was therefore foreseeable that the failure to adequately safeguard Financial Information would result in one or more of the following injuries to Plaintiffs and the members of the proposed Class: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the deep web black market;

expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

59. Accordingly, Plaintiffs, individually and on behalf of all those similarly situated, seek an order declaring that Wawa's conduct constitutes negligence and awarding damages in an amount to be determined at trial.

SECOND COUNT

NEGLIGENCE PER SE

On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, on Behalf of Plaintiffs and the Statewide Subclasses

60. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

61. Wawa violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect Financial Information and not complying with industry standards.

62. Wawa's violation of Section 5 of the FTC Act (and similar state statutes) constitutes negligence per se.

63. Class members are consumers within the class of persons Section 5 of the FTC Act (and similar state statutes) was intended to protect.

64. Moreover, the harm that has occurred is the type of harm the FTC Act (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable

data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiffs and the Class.

65. As a direct and proximate result of Wawa's negligence, Plaintiffs and Class Members have been injured and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

THIRD COUNT

BREACH OF IMPLIED CONTRACT

On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, on Behalf of Plaintiffs and the Statewide Subclasses

66. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

67. When Plaintiffs and Class Members paid money and provided their Financial Information to Wawa in exchange for goods or services, they entered into implied contracts with Wawa pursuant to which Wawa agreed to safeguard and protect such information and to timely and accurately notify them if their data had been breached and compromised.

68. Wawa solicited and invited prospective customers to provide their Financial Information as part of its regular business practices. These individuals accepted Wawa's offers and provided their Financial Information to Wawa. In entering into such implied contracts, Plaintiffs and the Class assumed that Wawa's data security practices and policies were reasonable and consistent with industry standards, and that Wawa would use part of the funds received from Plaintiffs and the Class to pay for adequate and reasonable data security practices.

69. Plaintiffs and the Class would not have provided and entrusted their Financial Information to Wawa in the absence of the implied contract between them and Wawa to keep the information secure.

70. Plaintiffs and the Class fully performed their obligations under the implied contracts with Wawa.

71. Wawa breached its implied contracts with Plaintiffs and the Class by failing to safeguard and protect their Financial Information and by failing to provide timely and accurate notice that their personal information was compromised as a result of a data breach.

72. As a direct and proximate result of Wawa's breaches of their implied contracts, Plaintiffs and the Class sustained actual losses and damages as described herein.

FOURTH COUNT

DISTRICT OF COLUMBIA CONSUMER SECURITY BREACH NOTIFICATION ACT, D.C. CODE §§ 28-3851, *et seq.*

On Behalf of Plaintiff Sacks and the District of Columbia Subclass

73. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

74. Wawa is a business that owns or licenses computerized data that includes "personal information," as defined by D.C. Code § 28-3852(a).

75. Plaintiffs and Class Members' Financial Information includes "personal information" as defined by D.C. Code § 28-3851(3).

76. Wawa is required to accurately notify Plaintiffs and Class Members if it becomes aware of a breach of its data security system in the most expedient time possible and without unreasonable delay under D.C. Code § 28-3852(a).

77. Because Wawa was aware of a breach of its security system, Wawa had an obligation to disclose the data breach in a timely and accurate fashion as mandated by D.C. Code § 28-3852(a).

78. By failing to disclose the Data Breach in a timely and accurate manner, Wawa violated D.C. Code § 28-3852(a).

79. As a direct and proximate result of Wawa's violations of D.C. Code § 28-3852(a), Plaintiffs and Class Members suffered damages, as described above.

80. Plaintiffs and Class Members seek relief under D.C. Code § 28-3853(a), including actual damages.

FIFTH COUNT

**DISTRICT OF COLUMBIA CONSUMER PROTECTION PROCEDURES ACT,
D.C. CODE §§ 28-3904, et seq.**

On Behalf of Plaintiff Sacks and the District of Columbia Subclass

81. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

82. Wawa is a "person" as defined by D.C. Code § 28-3901(a)(1).

83. Wawa is a "merchant" as defined by D.C. Code § 28-3901(a)(3).

84. Plaintiffs and Class Members are "consumers" who purchased or received goods or services for personal, household, or family purposes, as defined by D.C. Code § 28-3901.

85. Wawa advertised, offered, or sold goods or services in the District of Columbia and engaged in trade or commerce directly or indirectly affecting the people of the District of Columbia.

86. Wawa engaged in unfair, unlawful, and deceptive trade practices, misrepresentations, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of goods and services in violation of D.C. Code § 28-3904, including:

- a. Representing that goods or services have characteristics that they do not have;

- b. Representing that goods or services are of a particular standard, quality, grade, style, or model, when they are of another;
 - c. Misrepresenting a material fact that has a tendency to mislead;
 - d. Failing to state a material fact where the failure is misleading;
 - e. Advertising or offering goods or services without the intent to sell them as advertised or offered; and
 - f. Representing that the subject of a transaction has been supplied in accordance with a previous representation when it has not.
87. Wawa's unfair, unlawful, and deceptive trade practices include:
- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Class Members' Financial Information, which was a direct and proximate cause of the Data Breach;
 - b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
 - c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' Financial Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;
 - d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and Class Members' Financial Information, including by implementing and maintaining reasonable security measures;

- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' Financial Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;
- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Class Members' Financial Information; and
- g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' Financial Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

88. Wawa's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Wawa's data security and ability to protect the confidentiality of consumers' Personal Information.

89. Wawa intended to mislead Plaintiffs and Class Members and induce them to rely on its misrepresentations and omissions.

90. The above unfair and deceptive practices and acts by Wawa were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiffs and Class Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

91. Wawa acted intentionally, knowingly, and maliciously to violate the District of Columbia's Consumer Protection Procedures Act, and recklessly disregarded Plaintiffs' and Class Members' rights.

92. As a direct and proximate result of Wawa's unfair, unlawful, and deceptive trade practices, Plaintiffs and Class Members have suffered and will continue to suffer injury,

ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Wawa as they would not have paid Wawa for goods and services or would have paid less for such goods and services but for Wawa's violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their Financial Information; and an increased, imminent risk of fraud and identity theft.

93. Plaintiffs and Class Members seek all monetary and non-monetary relief allowed by law, including actual damages, restitution, injunctive relief, punitive damages, attorneys' fees and costs, the greater of treble damages or \$1,500 per violation, and any other relief that the Court deems proper.

SIXTH COUNT

VIOLATION OF THE NEW JERSEY CONSUMER FRAUD ACT, N.J.S.A. § 56:8-1, et seq. On Behalf of Plaintiff Katz and the New Jersey Subclass

94. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

95. The New Jersey Consumer Fraud Act (the "NJCFA"), N.J.S.A. § 56:8-1, et seq., prohibits the act, use or employment by any person of any unconscionable commercial practice, deception, fraud, false pretense, false promise, misrepresentation, or the knowing, concealment, suppression or omission, in connection with the sale or advertisement of any merchandise. The NJCFA applies whether or not any person has in fact been misled, deceived or damaged thereby. N.J.S.A. § 56:8-2.

96. Plaintiffs, Wawa, and Class Members are “persons” within the meaning of N.J.S.A. § 56:8-1(d).

97. Wawa sells “merchandise,” as defined by N.J.S.A. § 56:8-1, by offering convenience store goods and services to the public.

98. Wawa, operating in New Jersey, engaged in unconscionable and deceptive acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of convenience store goods and services in violation of N.J.S.A. § 56:8-2, including but not limited to the following:

- a. Misrepresenting material facts, pertaining to the sale of convenience store goods and services, to Plaintiffs and Class Members by representing that it would maintain adequate data security practices and procedures to safeguard Plaintiffs’ and Class Members’ Financial Information from unauthorized disclosure, release, data breaches, and theft;
- b. Misrepresenting material facts, pertaining to the sale of convenience store goods and services, to Plaintiffs and Class Members by representing that it did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Plaintiffs’ and Class Members’ Financial Information;
- c. Knowingly omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for Plaintiffs’ and Class Members’ Financial Information with the intent that Plaintiffs and Class Members rely on the omission, suppression, and concealment;

- d. Engaging in unconscionable and deceptive acts and practices with respect to the sale of convenience store goods and services by failing to adequately monitor and audit the data security systems of its vendors and business associates and failing to maintain the privacy and security of Plaintiffs and Class Members in violation of duties imposed by and public policies reflected in the FTC Act;
- e. Engaging in unconscionable and deceptive acts and practices by failing to disclose the Data Breach to Plaintiffs and Class Members in a timely and accurate manner in violation of N.J.S.A. § 56:8-163;
- f. Advertising Wawa's goods and services with the intent not to sell it as advertised – i.e., with worse data security than advertised; and
- g. Representing on its website that it is “is fully committed to data security” when, in fact, Wawa failed to safeguard customers’ information by relying on deficient data security protection.

99. The above unlawful and deceptive acts and practices by Wawa were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to consumers that the consumers could not reasonably avoid. This substantial injury outweighed any benefits to consumers or to competition.

100. Wawa knew or should have known that its data security practices were inadequate to safeguard Plaintiffs’ and Class Members’ Financial Information and that the risk of a data breach was highly likely. Wawa’s actions in engaging in the above-listed unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiffs and Class Members.

101. Plaintiffs and Class Members reasonably expected that Wawa would protect their Financial Information and reasonably expected that Wawa would provide truthful statements on its website and privacy policies, and that it would be safe to provide Wawa with their information. These representations and affirmations of fact made by Wawa, and the facts it concealed or failed to disclose, are material facts that were likely to deceive reasonable consumers, and that reasonable consumers would, and did, rely upon in deciding whether or not to provide their information to Wawa. Wawa, moreover, intended for consumers, including Plaintiffs and Class Members, to rely on these material facts.

102. As a direct and proximate result of Wawa's unconscionable and deceptive acts and practices, Plaintiffs and Class Members suffered an ascertainable loss in moneys or property, real or personal, as described above, including the loss of their legally protected interest in the confidentiality and privacy of their Financial Information.

103. Plaintiffs and Class Members seek relief under N.J.S.A. § 56:8-19, including but not limited to, injunctive relief, other equitable relief, actual damages, treble damages, and attorneys' fees and costs.

SEVENTH COUNT

VIOLATION OF THE NEW JERSEY CUSTOMER SECURITY BREACH DISCLOSURE ACT, N.J.S.A. §§ 56:8-163, et seq. On Behalf of Plaintiff Katz and the New Jersey Subclass

104. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

105. Wawa is a business that conducts business in New Jersey under N.J.S.A. § 56:8-163(a).

106. Plaintiffs' and Class Members' Financial Information includes personal information covered under N.J.S.A. §§ 56:8-163, et seq.

107. Under N.J.S.A. § 56:8-163(a), “[a]ny business that conducts business in New Jersey. . . shall disclose any breach of security of [] computerized records following discovery or notification of the breach to any customer who is a resident of New Jersey whose personal information was, or is reasonably believed to have been, accessed by an unauthorized person.”

108. Because Wawa discovered a breach of its security system involving the Financial Information of Plaintiffs and Class Members, in which such Financial Information was, or is reasonably believed to have been, acquired by an unauthorized person, and the Financial Information was not secured, Wawa had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated under N.J.S.A. §§ 56:8-163, et seq.

109. By failing to disclose the Data Breach in a timely and accurate manner, Wawa violated N.J.S.A. § 56:8-163(a).

110. As a direct and proximate result of Wawa's violations of N.J.S.A. § 56:8-163(a), Plaintiffs and Class Members suffered the damages described above.

111. Plaintiffs and Class Members seek relief under N.J.S.A. § 56:8-19, including treble damages, attorneys' fees and costs, and injunctive relief.

EIGHTH COUNT

VIOLATION OF THE VIRGINIA PERSONAL INFORMATION BREACH NOTIFICATION ACT, VA. CODE. ANN. §§ 18.2-186.6, et seq. On Behalf of Plaintiff Garthwaite and the Virginia Subclass

112. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

113. Wawa is required to accurately notify Plaintiffs and Class Members following discovery or notification of a breach of its data security system if unencrypted or unredacted Financial Information was or is reasonably believed to have been accessed and acquired by an unauthorized person who will, or it is reasonably believed who will, engage in identify theft or another fraud, without unreasonable delay under Va. Code Ann. § 18.2-186.6(B).

114. Wawa is each an entity that owns or licenses computerized data that includes Personal Information as defined by Va. Code Ann. § 18.2-186.6(B).

115. Plaintiffs' and Class Members' Financial Information includes Personal Information as defined by Va. Code Ann. § 18.2-186.6(A).

116. Because Wawa discovered a breach of its security system involving the Financial Information of Plaintiffs and Class Members that Wawa stored, in which unencrypted or unredacted Personal Information was or is reasonably believed to have been accessed and acquired by an unauthorized person, who will, or it is reasonably believed who will, engage in identify theft or another fraud, Wawa had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Va. Code Ann. § 18.2-186.6(B).

117. By failing to disclose the Data Breach in a timely and accurate manner, Wawa violated Va. Code Ann. § 18.2-186.6(B).

118. As a direct and proximate result of Wawa's violations of Va. Code Ann. § 18.2-186.6(B), Plaintiffs and Class Members suffered damages, as described above.

119. Plaintiffs and Class Members seek relief under Va. Code Ann. § 18.2-186.6(I), including actual damages.

PRAAYER FOR RELIEF

WHEREFORE, Plaintiffs and Class Members demand judgment as follows:

- A. That the Court certify this action as a class action, proper and maintainable pursuant to Rule 23 of the Federal Rules of Civil Procedure; declare that Plaintiffs are proper class representatives; and appoint Plaintiffs' Counsel as Class Counsel;
- B. That the Court grant permanent injunctive relief to prohibit Wawa from continuing to engage in the unlawful acts, omissions, and practices described herein;
- C. That the Court award Plaintiffs and Class Members compensatory, consequential, and general damages in an amount to be determined at trial;
- D. That the Court order disgorgement and restitution of all earnings, profits, compensation, and benefits received by Wawa as a result of its unlawful acts, omissions, and practices;
- E. That the Court award statutory damages, trebled, and punitive or exemplary damages, to the extent permitted by law;
- F. That Plaintiffs be granted the declaratory relief sought herein;
- G. That the Court award to Plaintiffs the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses;
- H. That the Court award pre- and post-judgment interest at the maximum legal rate; and
- I. That the Court grant all such other relief as it deems just and proper.

JURY TRIAL DEMANDED

Plaintiffs, on behalf of themselves and others similarly situated, hereby request a jury trial, pursuant to Federal Rule of Civil Procedure 38, on any and all claims so triable.

Dated: January 3, 2020

Respectfully submitted,



Linda P. Nussbaum
Bart D. Cohen (PA 57606)
James Perelman (PA 318456)
NUSSBAUM LAW GROUP, P.C.
1211 Avenue of the Americas, 40th Floor
New York, NY 10036-8718
(917) 438-9102
lnussbaum@nussbaumpc.com
bcohen@nussbaumpc.com
jperelman@nussbaumpc.com

Michael E. Criden
Lindsey C. Grossman
CRIDEN & LOVE, P.A.
7301 SW 57th Court, Ste. 515
South Miami, FL 33143
(305) 357-9000
mcriden@cridenlove.com
lgrossman@cridenlove.com

Counsel for Plaintiffs and the Proposed Class